Cassandra Crossing/ iPhone, Android e il dito sul grilletto

(138)—Quando si strombazza l'apertura delle piattaforme e poi si alzano palizzate per scongiurare il rischio dell'implosione. Libertà…

Cassandra Crossing/ iPhone, Android e il dito sul grilletto

Figure 1:

(138)—Quando si strombazza l'apertura delle piattaforme e poi si alzano palizzate per scongiurare il rischio dell'implosione. Libertà? Flessibilità? Il colpo è in canna.

24 ottobre 2008—Avete presente quella famosa litografia di M.C. Escher, "Galleria di quadri"?

E' interessante come qualche volta accada che cercare il centro di una questione complessa porti in evidenza un punto del "quadro" che avevi sempre trascurato e che sembrava un dettaglio secondario.

Il "quadro" del mondo IT attuale che per me aveva dell'inesplicabile era l'apparente protervia con cui i produttori, aspiranti o consolidati, di telefonini intelligenti e dei relativi kit di sviluppo di applicazioni li chiudevano a colpi di licenze, NDA e trucchetti software, "difendendoli" ad oltranza ed in maniera sorprendente.

Lo fanno da sempre Microsoft e Nokia con le loro piattaforme, lo fa fin dall'inizio Apple con iPhone, lo ha cominciato a fare Google con Android, sembra quindi essere un orientamento comune.

Oltretutto queste ultime aziende hanno anche ammesso l'inserimento di meccanismi software per la censura di applicazioni sgradite ai produttori.

Sembra di sentire nuovamente la protervia delle major dell'intrattenimento, come nel famoso caso Sony/BMG. Il fatto sorprende, visto che si tratta di oggetti che apparentemente avevano la loro forza nell'essere "aperti" e nell'attrarre sviluppatori e nuove applicazioni.

Oggetti che vengono relegati nel ghetto del software proprietario, un ghetto talvolta dorato ma che tarpa la crescita. C'è un problema, una apparente contraddizione, ci sono indizi probabilmente essenziali, ma niente di conclusivo. Spostiamoci allora nel campo della sicurezza.

Qui in effetti, a chi abbia appena una infarinatura di architettura di applicazioni, appare evidente che una importante infrastruttura di servizi, la telefonia mobile, viene messa in discussione (anzi stravolta) dalla comparsa di client intelligenti e completamente programmabili.

I terminali di telefonia mobile (telefonini) programmabili dall'utente introducono dall'oggi al domani nell'infrastruttura di un provider di telefonia mobile un enorme problema di sicurezza. La gestione della sicurezza di una infrastruttura GSM/UMTS è infatti costituita prima di tutto da "security throught obscurity" e da componenti hardware/software proprietarie e tenute il più possibile segrete e non modificabili dall'utente-proprietario.

Con questo modello (inesistente) di sicurezza, "aprire" completamente la parte dei terminali utente (i telefonini) equivarrebbe ad una condanna a morte rapida e dolorosa di tutta l'infrastruttura. Per sopravvivere diverrebbe vitale implementare, ma soprattutto gestire, un layer di protezione dell'infrastruttura dai suoi stessi terminali, divenuti potenzialmente erratici od ostili perché liberamente modificabili.

Il problema dei terminali ostili è amplificato a dismisura dall'assoluta omogeneità di percentuali significative dei terminali stessi.

Chi si occupa di sicurezza del software parla di "omogeneità genetica" come di un fattore che, analogamente a quanto avviene nei sistemi biologici, diminuisce la resistenza ai virus ed aumenta la possibilità di una infezione inarrestabile e fatale. Il problema è salito alla ribalta delle cronache con la prevalenza del sistema operativo Windows, che offre un terreno fertile ed omogeneo per virus ed attacchi informatici di vario tipo proprio perché rende simili ed omogenei la maggior parte dei PC al mondo.

Gli iPhone, per fare l'esempio più famoso, sono quasi perfettamente uguali tra loro; così i vari tipi di terminali Nokia e di altri produttori: anche tra modelli esternamente assai diversi il software di sistema è molto omogeneo.

Come e peggio che nel caso di Windows, una singola vulnerabilità in un modello popolare di terminale GSM potrebbe permettere ad un programma malevolo (costituito o contenente un virus o un worm) di diffondersi e compromettere tutti i terminali di quel tipo a velocità elevatissime, molto superiori a quelle dei normali virus e worm da PC e probabilmente simili a quella del noto SQL Slammer.

I cellulari moderni infatti potenziano moltissimo la connettività tra terminali. Due telefonini moderni possono colloquiare tra loro in modalità "normale" GPRS/UMTS, ma anche via rete Bluetooth con apparecchiature di tipo diverso, e via rete WiFi con altri apparecchi ed intere reti.

Pensate quante modalità di infezione contemporanee possono essere utilizzate da un programma malevolo che giri su un cellulare per riprodursi.

E se dopo la diffusione ogni virus cominciasse a telefonare a numeri erotici? Pochi lo sanno, ma un telefonino può attivare fino ad 8 conversazioni fonia e dati contemporanee ed indipendenti. Potrebbe ad esempio quasi azzerarvi la ricarica mentre sta nella vostra tasca, verificando anche di lasciarvi qualche cosa perché non ve ne accorgiate subito.

E se alcune centinaia di migliaia di telefonini chiamassero contemporaneamente? Questo saturerebbe la rete di qualunque provider, azzerando la possibilità di effettuare chiamate legittime, quindi i ricavi del provider stesso e probabilmente anche le sue quotazioni in borsa.

Ecco forse abbiamo trovato il bandolo! I soldi, o meglio la paura di perderli.

E' perfettamente comprensibile che chi produce telefonini intelligenti e programmabili voglia contrastare questa eventualità, a costo di fare cose che abbassino l'appetibilità del prodotto, ed a maggior ragione la sua "moralità" o "popolarità". Se poi il produttore fosse restio a prendere queste misure, ci penserebbero i provider di telefonia mobile a costringerli (come accaduto nelle trattative americane tra Apple ed AT&T).

Ecco però che si manifesta la stessa forma di "idiozia" che caratterizza spesso i comportamenti delle aziende, perché sono fatti di ottimizzazioni e risposte a problemi locali, che di frequente allontanano dalla soluzione ottima e producono mostri tecnologici "globalmente" sbagliati.

Infatti, prendendo ancora ad esempio Apple che, si noti, non ha più torti di altri ma semplicemente una storia più lunga e più nota, è stata implementata una blacklist in cui il sistema operativo del telefonino periodicamente consulta un sito web che contiene un elenco di applicazioni (con hash e altre informazioni) che permette di verificare se un qualche eseguibile che sta girando sul terminale è malevolo: il sistema operativo tira il grilletto della pistola che possiede, stoppa il processo e cancella l'eseguibile.

Funziona tutto in teoria, anche se non esiste nessuna garanzia che chi ha il dito sul grilletto (in questo caso Apple) lo schiacci solo se vede un virus, visto che la tentazione di usarlo, in maniera più o meno esplicita contro, ad esempio, un concorrente commerciale sarebbe forte.

Inoltre, ed è il fatto più grave, questo costituisce una limitazione a priori della libertà tanto strombazzata degli utenti e degli sviluppatori.

E' sempre utile ricordare che non esiste una "libertà limitata" proprio come non esiste una "ragazza quasi incinta".

Infine, ed è la strada che conduce al baratro, **questa è la risposta tecnologica sbagliata al problema**.

Chi scrive virus, opera quotidianamente la sovversione di tecniche semplici di protezione come questa. I virus polimorfi ad esempio, noti da oltre un decennio, non sarebbero rilevabili da un tale sistema, e comunque aggirare un sistema noto e statico di protezione è il pane quotidiano di chi scrive software malevolo.

La sicurezza aggiuntiva per una rete GSM fornita da una patch come questa è probabilmente vicina allo zero, ed un attacco distruttivo di grossa portata resta sempre possibile.

La risposta giusta, ma costosa e difficile, sarebbe ovviamente riprogettare l'infrastruttura insicura rendendola sicura, senza dover ingabbiare i telefonini ed i relativi utenti, e guadagnando in sicurezza reale invece che immaginaria.

Nel frattempo, come sempre, ci rimettono gli utenti-consumatori, che pagano il prezzo della (in)sicurezza delle scelte sbagliate sia in termini monetari che di libertà e flessibilità di uso.

Ovviamente, con buona pace del progresso e del libero mercato.

Originally published at punto-informatico.it.